Nginx 服务器“秘籍”

文 / 刘旻昊

新采编发系统是由新华社技术局主持研发，服务于新华社全社新闻采编报道日常业务的新一代新闻采编系统，是 2016 年实施的新华全媒工程的重要组成，该系统提供信息汇聚、报道策划、全媒生产、产品发布等四大类主要功能。面对业务需求变化快、运维工作日趋复杂、IT 运维技术换代快等挑战，按照“要遵循新闻传播规律和新兴媒体发展规律，运用互联网技术体系，提升技术人员对先进技术的自主掌控能力”的。

这就是新华全媒工程选择 Nginx 作为 Web 服务器的主要原因。作为一个草根出身的软件，Nginx 在业界的鼎鼎大名也许你并不陌生。十多年前，它刚一诞生就出手不凡，很好地解决了传统 Web 服务器 Apache 无法 hold 住的 C10K 的问题（即一台物理服务器达到并发量 1 万的时候，Apache 就会承受不了）。

如今，在新华社新一代技术系统架构中，Nginx 作为接入层的重要环节扮演了至关重要的角色，通过自主掌控 Nginx 软件的安装配置，灵活运用各种内置、第三方模块及自定义 lua 脚本，不仅可以完成基本的代理转发和软负载，还能通过对流量的多种控制处理实现认证鉴权、SSL 卸载、限速分流、接入审计等功能，以满足用户和应用系统的多种需求。

Nginx 是一款开源免费的 HTTP 和反向代理服务器，它由俄罗斯人伊戈尔·塞索耶夫编写，最早发布于2004年。十多年来，由于其出色的性能，Nginx 在互联网突飞猛进的时代里飞速发展，根据 W3Techs 网站的报告，目前全球 TOP 1000 的网站中有接近六成在使用 Nginx，包括 Netflix, Dropbox, Wikipedia 等，而排名第二的 Apache 仅占 16.5%。Nginx 最突出的特性包括高并发、轻量级、稳定，这得益于它使用异步、非阻塞、事件驱动的方式处理请求，测试显示它能处理高达Apache4倍之多的并发请求量，同时使用的内存资源却远低于 Apache。

要使用 Nginx，第一步要掌握 Nginx 的安装：

在安装 Nginx 之前，首先要安装 3 个依赖软件包：PCRE 正则表达式库，zlib 压缩库和 OpenSSL 加密工具集，Nginx 的配置、压缩和 ssl 功能中需要用到这些软件。

安装 Nginx 包括 3 步，配置、编译和安装，首先需要在 Nginx 官网 http://nginx.org/ 下载源码包，一般建议使

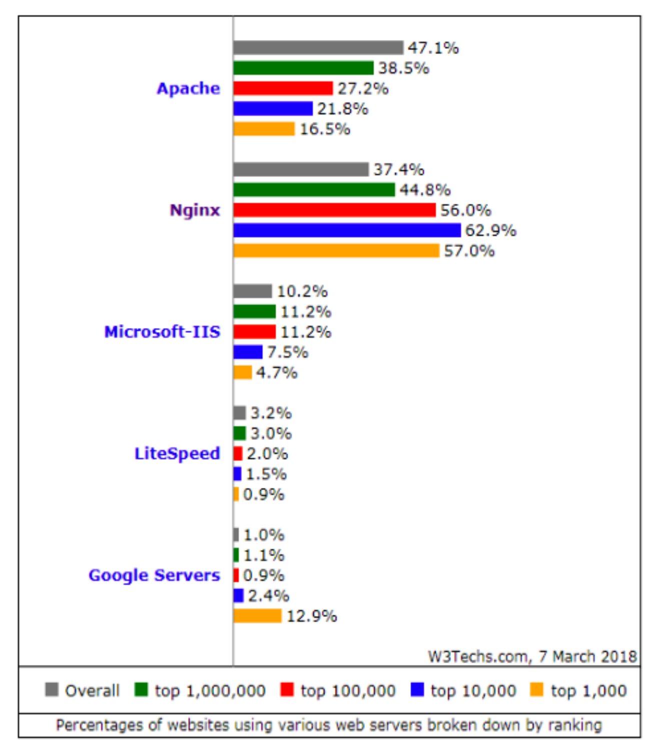


图 1　全球 Web 服务器排名

用稳定版（Stable Version）。

在配置阶段，由于 Nginx 使用高度模块化的架构设计，需要手动设置各个模块的开关选项。对于默认关闭的 Nginx 内置模块，可以使用 --with-module_name 的方式开启开关，对于第三方模块，可以使用 --add-module=/path/to/module 的方式加以集成。

启用一些常用的内置模块的配置如下：

- --with-stream　　四层协议转发
- --with-http_ssl_module　　支持 https
- --with-http_gzip_static_module Gzip　静态模块
- --with-http_geoip_module　GeoIP　　模块
- --with-http_flv_module　　为 FLV 文件提供服务端伪流媒体支持
- --with-http_stub_status_module　　状态信息页

Nginx 有大量的第三方模块，官网上提供了所有第三方模块的清单：https://www.nginx.com/resources/wiki/modules/index.html，一些常用的第三方模块包括：

- nginx_upstream_check_module　　主动健康检查
- nginx-sticky-module　　会话保持

- ngx_log_if 日志过滤

使用 make 和 make install，就完成编译安装了。

安装完成后，还需要掌握 Nginx 的基本控制命令：

- nginx 启动 nginx
- nginx –s stop 立刻停止
- nginx –s quit 温柔停止
- nginx –s reload 重载配置文件

了解完安装和基本控制，来看看 Nginx 具体能扮演哪些角色吧：

1. 反向代理

应用部署好了，如何让用户能访问到呢？这正是 Nginx 反向代理的用武之地，用户通过域名访问的请求到达 Nginx 服务器后，Nginx 可以根据域名和路径区分这些请求并转发给不同的后端服务器集群，即使用户无法通过网络直达这些后端服务器。Nginx 四层和七层的代理分别使用 ngx_stream_proxy_module 和 ngx_http_proxy_module 模块，都用 proxy_pass URL 的方式配置实现。

2. 负载均衡

应用服务器出问题了怎么办？不要紧，将 Nginx 用做软负载，能够将影响程度降低至最低。Nginx 可以提供灵活多变的负载配置，包括轮询、加权轮询、IP 哈希、主备等，用于满足多样的需求。此外，还可以通过集成 nginx_upstream_check_module 第三方模块，进一步实现基于 tcp 和 http 的主动健康检查，让 Nginx 的负载均衡能力如虎添翼。

3. 访问控制

并非所有的系统都全部面向互联网开放，有的系统只允许办公网络访问，还有的系统里某些页面可以对互联网开放，其他页面则仅允许特定的内部 IP 访问，面对这些细粒度的访问控制需求，通过使用 ngx_http_access_module 模块，Nginx 可以提供基于七层的灵活的黑白名单方式配置访问控制策略。

4. 认证鉴权

有些应用系统想要加把锁，输入正确的用户名密码才能访问，nginx 默认自带的认证模块就可以实现，通过 ngx_http_auth_basic_module 模块，结合 htpasswd 命令生成用户名及对应密码数据库文件，Nginx 可以很轻松地实现这种认证。另一种认证方式也很流行，Nginx+Lua（类似 Openresty）可以让用户在访问业务系统之前先通过统一的用户认证系统登录、过滤并鉴权。

5. SSL 卸载

近年来，HTTPS 逐渐取代 HTTP 成为传输协议界的新宠，众多互联网网站开始从 HTTP 切换到 HTTPS，以实现加密、可信访问。Nginx 的 ngx_http_ssl_module 模块对 https 提供了必要的支持，想要实施 HTTPS 的网站可以将证书安装在 Nginx 服务器上，由 Nginx 进行 ssl 密文数据流的卸载。

6. 限速限流

当遇到真实的流量远远大于系统测试的可承载流量时，一方面可能让系统垮掉，另一方面可能拥堵出口带宽，这时就必须进行限流。限流是从上到下贯穿整个应用的，接入层作为最外面的屏障，需要做好整个系统的限流。对于 Nginx 来讲，限流有多种方式，可以使用 ngx_http_core_module 核心模块对连接数进行限制，也可以对访问频率进行限制，还可以启用过载保护 sysgurad 模块。

7. 接入审计

可以通过搭建 ELK 平台收集和分析接入层 Nginx 日志，实现可视化的接入审计及分析平台，消息队列可以采用 Redis 或 Kafka。

除了上述种种应用场景，Nginx 还有一个运维人员不可不知的炫酷操作——平滑升级。作为一个互联网软件，Nginx 版本迭代升级比较频繁，对运维人员来说，为了享受新版本的新特性，免不了要对生产环境的 Nginx 进行版本升级，而平滑升级操作可以在业务毫无感知的情况下完成，运维人员只需在备份并替换 sbin 目录下的可执行文件后，使用 kill –s USR2 `cat /path/to/nginx.pid` 命令，让 Nginx 开始新旧版本并行运行，随后再优雅退出旧进程即可。

看到这里，你有没有跃跃欲试了呢，快去体验一下这款 Web 服务器神器吧。

（作者单位：新华社通信技术局）